The opinion in support of the decision being entered today was *not* written for publication and is *not* binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte TERRY MICHAEL BLEIZEFFER, MARK DAVID GILMORE, and MARTIN JOSEPH CLAYTON PRESLER-MARSHALL

Appeal No. 2006-2354
Application No. 09/877,157
Technology Center 3600

ON BRIEF

Before LEVY, NAPPI and HORNER, *Administrative Patent Judges.*

HORNER, *Administrative Patent Judge.*

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134(a) from the examiner's final rejection of claims 1-24, all of the claims pending in the application.

We affirm.

BACKGROUND

The appellants' invention relates to a method, apparatus, interface, and computer program product for creating a privacy policy. Claims 1 and 23, reproduced below, are exemplary of the subject matter on appeal.

> 1. A data processing apparatus-implemented method for creating a privacy policy, comprising data processing apparatus-implemented steps of:
>
> creating a policy group;
>
> moving a data element to the policy group; and
>
> generating a privacy policy based on the policy group.
>
> 23. An interface for creating a privacy policy, comprising:
>
> a first portion for displaying predefined data elements;
>
> a second portion for displaying groups of data elements, wherein a group of data elements shares at least one common property; and
>
> a third portion for displaying a privacy policy generated from the groups of data elements.

A copy of all of the claims on appeal can be found in the appendix to the appellants' brief.

The examiner relies upon the following as evidence of unpatentability:

Abraham *et al.* (Abraham)	WO 98/40987	Sep. 17, 1998
Moriconi *et al.* (Moriconi)	6,158,010	Dec. 05, 2000

The appellants seek our review of the examiner's rejection of claims 1-24 under 35 U.S.C. § 103(a) as being unpatentable over Moriconi in view of Abraham.

Rather than reiterate in detail the conflicting viewpoints advanced by the examiner and the appellants regarding this appeal, we make reference to the examiner's answer (mailed February 3, 2006) for the examiner's complete reasoning in support of the rejection and to the appellants' brief (filed January 31, 2005) and reply brief (filed March 31, 2006) for the appellants' arguments.

OPINION

In reaching our decision in this appeal, we have carefully considered the appellants' specification and claims, the applied prior art, and the respective positions articulated by the appellants and the examiner. As a consequence of our review, we affirm the examiner's rejection of claims 1-24 under 35 U.S.C. § 103(a).

Only those arguments actually made by the appellants have been considered in this decision. Arguments that the appellants could have made but chose not to make in the brief have not been considered. We deem such arguments to be waived by the appellants. *See* 37 C.F.R. § 41.37(c)(1)(vii) (2006).

Findings of Fact

With regard to the scope and content of the prior art, we make the following findings of fact:

1. Moriconi discloses a method for creating a security policy that includes creating a policy group, moving a data element to a policy group, and generating a security policy based on the policy group.

2. In particular, Moriconi describes a process for creating and customizing rules to manage a security policy from a centralized server in a distributed computer network. Moriconi, col. 3, lines 50-54 and 57-63 and col. 4, lines 19-22.
3. Moriconi discloses that an administrator can use a policy manager to create a global policy that specifies access privileges of the user to securable components of the network. Moriconi, col. 4, lines 25-26.
4. The policy manager allows privileges to be grouped together and granted to a named role such as a set of privileges needed to perform a job function. Moriconi, col. 7, lines 49-58.
5. Moriconi discloses that the administrator may add global roles (912) and local roles (916) on a server or client using the policy manager (210), thereby teaching that the administrator can create policy groups. Moriconi, col. 12, lines 35-39, see also col. 12, lines 55-61.
6. In this case, the data elements in Moriconi are the individual privileges. These data elements (privileges) are combined into a named group (based on a role), which has been defined by the administrator creating the security policy. The security policy is then generated based on these groups (by assigning the privileges associated with that role to the designated user(s)).
7. The policy manager also allows different users to be grouped together. Moriconi, col. 6, lines 28-29.
8. For example, Moriconi teaches that "[u]sers granted to a role are the members of that role." Moriconi, col. 7, lines 56-57.

9. In this example, the data elements in Moriconi are the individual users. These data elements (users) are combined into a named group (corresponding to a role) that is defined by the administrator. The security policy is then generated based on these groups by assigning certain privileges to the users within the named group. Moriconi, col. 7, lines 42-54 and col. 9, lines 61-63.

10. The data elements (users) in the group, as in the claimed invention, all share common properties, *viz,* they share the same role or job.

11. Moriconi teaches a parser/type checker that reviews and reconstructs the policy rules to check for errors by making sure that the rules are syntactically and semantically correct according to a predefined policy language. Moriconi, col. 9, line 66 – col. 10, line 3 and col. 11, lines 44-47.

12. Moriconi further teaches maintaining an audit log that is accessible by the administrator via a log viewer in the management station. Moriconi, col. 11, lines 33-34.

13. Abraham similarly discloses a method for creating a security policy that includes creating a policy group, adding data elements to the group, and generating a security policy based on the group.

14. Specifically, the system of Abraham discloses a method for a system administrator to set specific policies for the users of a local area network regarding what type of services and information each user may access on the Internet. Abraham, page 8, lines 4-6.

15. The system administrator uses a graphical user interface to set policies for each user and information about the policies is stored in tables in a database. Abraham, page 10, lines 20-22; see also page 12, lines 10-13.

16. Abraham discloses allowing system administrators to group users of the LAN together. Abraham, page 14, lines 30-32.

17. The system administrator can create ("add") subgroups to a root group and then move the data elements ("add users as members") to the subgroup via the graphical user interface. Abraham, page 15, lines 8-13; see also page 29, lines 19-27.

18. Abraham teaches that the user inherits all of the policies and quotas of the group to which it has become a member. Abraham, page 30, lines 2-3.

19. After the system administrator has added a new group, a record for the group is added to a user group table in a database. Abraham, page 28, lines 3-5.

20. A record for a user is added to a transmit list stored in a database and is used to construct a user policy table that is ultimately provided to the filter executive. Abraham, page 24, lines 25-32.

21. A filter executive loads the policies for each user from the database and generates a policy ("set of rules") for each user. These rules are used by the filter engine to block unauthorized services or information. Abraham, page 10, lines 32-34; see also page 13, lines 26-31 and Figures 15A-15C.

22. In this example, the data elements in Abraham are the individual users. These data elements (users) are combined into groups (e.g., subgroups of the root group comprised of all users). The policy is then generated based on the groups by designating a set of rules for a group to control access to certain information and services on the Internet.

23. Abraham describes a method for allowing a system administrator to set policies, e.g., file type policies that prevent groups and users from downloading certain types of files. Abraham, page 37, lines 7-10.

24. This policy becomes policy-wide when the administrator selects to apply it to the root group, *i.e.*, all users on the LAN. Abraham, page 14, lines 31-35.

25. The system of Abraham generates the policy based on the settings selected by the administrator. Abraham, page 41, lines 26-30.

26. Abraham discloses the step of generating a human-readable version of the policy. For example, when a system administrator sets a site policy that allows a group to access all sites with the exception of specified sites, or denies access to the group to all sites with the exception of specified sites, the policy is displayed to the administrator in human readable form in the site policy tab window, as shown in Figure 8O. Abraham, page 41, lines 17-30.

27. Abraham discloses the step of generating a table of policy elements. For example, when a system administrator sets a site policy that allows a group to access all sites with the exception of specified sites, or denies access to the group to all sites with the exception of specified

sites, the policy is displayed to the administrator in a table, as shown in Figure 8O. Abraham, page 41, lines 17-21.

28. Figure 6 of Abraham shows a graphical user interface (70) having a main window (84) with three portions. A first portion contains a list of predefined data elements (user list 88) that identifies all users of the LAN. Abraham, page 14, lines 14-15.

29. A second portion displays groups of data elements (group hierarchy 86). Abraham, page 14, line 32. In the example of Figure 6, the root of the hierarchy is a group containing all of the users identified in the user list (88), and the subgroups contain users corresponding to various departments of a corporation. Abraham, page 14, line 32 – page 15, line 4.

30. The users in the root group share at least one common property, because all of the users in the root group are employees of the corporation.

31. The users in the subgroups share at least one common property, because all of the users in a subgroup are members of a particular corporate department.

32. The interface (70) includes a third portion that displays the policy generated from the groups of data elements. In particular, Abraham teaches that the site policy tab (95) in the third portion of the window (84) can be used by the administrator to set site policies for a group in the group hierarchy (86). Abraham, page 41, lines 19-20.

33. When the administrator selects the site policy tab (95), a site policy tab window (145) is generated by the interface (70), as shown in Figure 8O. Abraham, page 41, lines 20-21.

34. When a system administrator sets a site policy that allows a group to access all sites with the exception of specified sites, or denies access to the group to all sites with the exception of specified sites, the generated policy is displayed to the administrator as a list of restricted sites in human-readable form, as shown in Figure 8O. Abraham, page 41, lines 26-30.

35. The appellants admit in the specification that the data elements of the P3P specification are already known in the prior art:

> The [prior art] P3P specification defines the syntax and semantics of P3P privacy policies and the mechanisms for associating policies with Web resources. P3P policies consist of statements made using the P3P vocabulary for expressing privacy practices. P3P policies also reference elements of the P3P base data schema – a standard set of data elements. The P3P specification includes a mechanism for defining new data elements and data sets and a simple mechanism that allows for extensions to the P3P vocabulary. (Specification, page 1, line 27 – page 2, line 3.)

36. Further, the recited step of "generating a privacy policy" is described in the specification as merely generating a list of all of the selected data elements in the policy. Specification, page 15, lines 28-30.

37. For example, the specification describes:

> [P]olicy pane 430 in Figure 4 shows a list of all the data elements in the policy. . . . This provides the user with an

> immediate description of the state of the policy. The list of data elements provides a summary of all data elements in the policy to allow the user to easily match up with, for example, a Web form that the policy may cover. (Specification, page 15, line 29 – page 16, line 6.)

Claims 1, 12, and 24

The appellants argue claims 1, 12, and 24 as a group. As such, we treat claim 1 as the representative claim. In rejecting claims under 35 U.S.C. § 103(a), the examiner bears the initial burden of establishing a prima facie case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). *See also In re Piasecki*, 745 F.2d 1468, 1472, 223 USPQ 785, 788 (Fed. Cir. 1984). The examiner can satisfy this burden by showing that some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references such that they would suggest or teach the claimed subject matter. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). Only if this initial burden is met does the burden of coming forward with evidence or argument shift to the appellant. *Oetiker*, 977 F.2d at 1445, 24 USPQ2d at 1444. *See also Piasecki*, 745 F.2d at 1472, 223 USPQ at 788.

In the rejection of independent claim 1, the examiner determined that Moriconi discloses a method for creating a privacy policy as claimed except that it does not explicitly disclose creating a policy group. The examiner relies on Abraham for the teaching of creating a policy group. The examiner found that it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of Moriconi with the method of Abraham in order to secure management of a computer network. Answer, p. 3.

To determine whether a prima facie case of obviousness has been established, we are guided by the factors set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966), *viz.*, (1) the scope and content of the prior art; (2) the differences between the prior art and the claims at issue; and (3) the level of ordinary skill in the art.[1]

Both prior art references teach or suggest the method steps of claim 1 except that the methods of the prior art are used to generate security policies instead of a privacy policy (see facts 1-10 and 13-22). As such, the claimed method merely provides a way to create a privacy policy using known method steps, as taught by Moriconi and Abraham, and using known data elements from the P3P specification (see fact 35).

The appellants contend that the examiner has failed to meet his initial burden of presenting a prima facie case of obviousness. Brief, p. 11 (citing *Oetiker*, 977 F.2d at 1445, 24 USPQ2d at 1444). Specifically, the appellants argue that neither Moriconi nor Abraham teach or suggest any type of privacy policy, or the creation of a privacy policy. Brief, pp. 11-12. The appellants contend that Moriconi is directed to ensuring that clients are authorized to access securable components by use of a security policy, and that security and privacy are different concepts such that the teaching of a security policy in Moriconi does not teach or suggest a privacy policy as claimed. Brief, p. 12. The appellants presented evidence demonstrating the differences between security and privacy policies and services. Brief, pp. 12-13 (discussing evidence in Appendices A-C). The appellants further

---

[1] Although *Graham* also suggests analysis of secondary considerations such as commercial success, long felt but unsolved needs, failure of others, etc., the appellants presented no such evidence of secondary considerations for the Board's consideration.

argue that even if Moriconi discloses enforcement of a privacy policy, claim 1 is not directed to enforcement, but rather it is directed to establishment or creation of a privacy policy. Brief, p. 14. As such, the appellants contend that the examiner has failed to establish any teaching or suggestion in the prior art of creating a privacy policy, or any step of creating a privacy policy based on a policy group. Brief, p. 14.

The question before us is whether the difference between using the claimed method to generate a list of data elements relating to privacy as opposed to a list of data elements relating to security would have been unobvious to one of ordinary skill in the art at the time the invention was made and thus patentable. In other words, the question before us is whether patentable weight should be accorded to the claim limitations that recite a "privacy" policy.

Functional versus non-functional descriptive material

Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." Exemplary "functional descriptive material" consists of data structures and computer programs, which impart functionality when employed as a computer component. "Nonfunctional descriptive material" includes but is not limited to music, literary works and a compilation or mere arrangement of data. If we find that the underlying privacy data elements used to generate the claimed privacy policy are nonfunctional descriptive material, then the question before us is whether a claim that differs from the prior art solely as to non-functional descriptive material is unobvious under 35 U.S.C. § 103. Although no issue under 35 U.S.C. § 101 is before this Board, the decisions of our reviewing courts on this issue provide useful guidance with respect

to (a) distinctions between "functional" and "non functional" descriptive material, and (b) how the distinctions impact the courts' treatment of each type of descriptive material.

Functional descriptive material

When functional descriptive material is recorded on a computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. *Compare In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994) (claim to data structure stored on a computer readable medium that increases computer efficiency held statutory) *with In re Warmerdam*, 33 F.3d 1354, 1361-62, 31 USPQ2d 1754, 1759-60 (Fed. Cir. 1994) (claim to computer having a specific data structure stored in memory held statutory product-by-process claim but claim to a data structure that referred to ideas reflected in nonstatutory process rather than referring to a physical arrangement of the contents of a memory held nonstatutory).

Non-functional descriptive material

When nonfunctional descriptive material is recorded on a computer-readable medium, in a computer or on an electromagnetic carrier signal, it is not statutory because no requisite functionality is present to satisfy the practical application requirement. Merely claiming nonfunctional descriptive material, i.e., abstract ideas, stored in a computer-readable medium, in a computer, on an electromagnetic carrier signal does not make it statutory. *See Diamond v. Diehr*, 450 U.S. 175, 185-86, 209 USPQ 1, 7-8 (1981) (noting that the claims for an algorithm in Benson were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose

computer.") Such a result would exalt form over substance. *In re Sarkar*, 588 F.2d 1330, 1333, 200 USPQ 132, 137 (CCPA 1978) ("[E]ach invention must be evaluated as claimed; yet semantogenic considerations preclude a determination based solely on words appearing in the claims. In the final analysis under 101, the claimed invention, as a whole, must be evaluated for what it is.") (*quoted with approval in In re Abele*, 684 F.2d 902, 907, 214 USPQ 682, 687 (CCPA 1982)). *See also In re Johnson*, 589 F.2d 1070, 1077, 200 USPQ 199, 206 (CCPA 1978) ("form of the claim is often an exercise in drafting"). Thus, nonstatutory music is not a computer component, and it does not become statutory by merely recording it on a compact disk. Protection for this type of work is provided under copyright law.

Prior art rejections and descriptive material

When presented with a claim including nonfunctional descriptive material, an Examiner must determine whether such material should be given patentable weight. The Patent and Trademark Office (PTO) must consider all claim limitations when determining patentability of an invention over the prior art. *In re Gulack*, 703 F.2d 1381, 1385, 217 USPQ 401, 404 (Fed. Cir. 1983). The PTO may not disregard claim limitations comprised of printed matter. *See Gulack*, 703 F.2d at 1384, 217 USPQ at 403; *see also Diamond v. Diehr*, 450 U.S. at 191, 209 USPQ at 10. However, the PTO need not give patentable weight to descriptive material absent a new and unobvious functional relationship between the descriptive material and the substrate. *See Gulack,* 703 F.2d at 1386, 217 USPQ at 404. *See also In re Ngai*, 367 F.3d 1336, 1338, 70 USPQ2d 1862, 1863-64 (Fed. Cir. 2004); *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994). The

burden of establishing the absence of a novel, nonobvious functional relationship rests with the PTO. *Lowry*, 32 F.3d at 1584, 32 USPQ2d at 1034.

We conclude that when the prior art describes all of the claimed structural and functional relationships between descriptive material and the substrate, but the prior art describes a different descriptive material than the claim, then the claimed descriptive material is non-functional and will not constitute a sufficient difference from the prior art to establish patentability. That is, we conclude that such a scenario presents no new and unobvious functional relationship between the descriptive material and the substrate.

We hold that the Platform for Privacy Preferences (P3P) data elements used in the method to generate a privacy policy do not functionally change the data processing apparatus-implemented method, because they do not alter how the process steps are to be performed to achieve the utility of the invention. Rather, these data elements are analogous to printed matter in that they represent merely underlying data in a database. *See Lowry*, 32 F.3d at 1583, 32 USPQ2d at 1034. In particular, as we found above, the prior art suggests using the claimed method steps to create a security policy using, for example, the data elements of users and/or privileges (see facts 1-10 and 13-22). The present invention uses these same method steps to create a privacy policy using the data elements from the known P3P data base schema (see fact 35). The difference between the prior art and the claimed invention is simply the starting data elements that result in generation of privacy policy as opposed to a security policy. These starting data elements neither enhance nor diminish the functionality of the steps used to generate the policy.

The step of generating a *privacy* policy is described in the specification as, for example, the creation of a human-readable list of all of the selected data elements in the policy (see facts 36, 37). As demonstrated by the teachings of Abraham (see facts 26, 34), a person having ordinary skill in the art at the time of the invention would have known how to take the policy groups and the selected data elements therein and generate a list of these data elements. The fact that the claimed data elements in the list relate to privacy, rather than security, does not present a patentable distinction, because the content of the data elements does not functionally relate to how the data elements are displayed or otherwise used or manipulated by the claimed method. As such, we sustain the examiner's rejection of claims 1, 12, and 24 as unpatentable under 35 U.S.C. § 103.

This case is distinguished from *Lowry*, because in *Lowry* the claims were directed to data structures stored in memory that contained both information used by application programs and *information regarding their physical interrelationships* within a memory. *Id.* As such, the court found that the claimed data structures of Lowry's invention were not analogous to printed matter because they managed information by imposing a physical organization on the data and provided increased computing efficiency. *Id.* By contrast, the present invention is directed to a method where the only distinction to the prior art is the content of the data elements. Unlike in *Lowry*, the data in the present case does not impose any functional requirements on the claimed method and the claimed method does not depend functionally on the information content of the data elements. Nonfunctional descriptive material cannot render nonobvious an invention that would have otherwise been obvious. *Ngai*, 367 F.3d at 1339, 70 USPQ2d at 1864. *Cf. Gulack*,

703 F.2d at 1385, 217 USPQ at 404 (when descriptive material is not functionally related to the substrate, the descriptive material will not distinguish the invention form the prior art in terms of patentability).

The appellants did not separately argue the patentability of the rejected dependent claims 2, 3, 8, 9, 13, 14, 19, and 20. Rather, the appellants relied on the arguments for patentability of claims 1 and 12. As such, we treat claims 2, 3, 8, 9, 13, 14, 19, and 20 as standing or falling together with their respective independent claims.

Claims 4 and 15

The appellants argue claims 4 and 15 as a group. We treat claim 4 as the representative claim. The appellants contend that none of the cited references suggest the claimed steps of updating a policy-wide property, and generating the privacy policy based on the policy-wide property. Brief, p. 15. We disagree and hold that Abraham teaches these steps (see facts 23-25). As such, we sustain the examiner's rejection of claims 4 and 15.

Claims 5 and 16

The appellants argue claims 5 and 16 as a group. We treat claim 5 as the representative claim. The examiner rejected claim 5 on the grounds that although Moriconi does not expressly teach the step of generating a human-readable version of the policy, it would have been obvious that if the policy is manipulated via a GUI that it would be readable to a user. Answer, p. 3. The appellants argue that none of the references teach or suggest this step. Brief, p. 16. We disagree with both the examiner and the appellants and find that the prior art, in fact, expressly teaches generating a human-readable version of the policy (see facts 26 and 34). Accordingly, we sustain the rejection of claims 5 and 16 under 35 U.S.C. § 103(a).

Claims 6, 7, 17, and 18

The appellants argue claims 6, 7, 17, and 18 as a group. We treat claims 6 and 7 as representative claims. Claims 6 and 7 recite that the human readable version of the policy is an HTML or XML version, respectively. The examiner took Official Notice that generating a "hypertext markup language version of the policy" or "an extensible markup language version of the policy" is common and well known in the prior art in reference to policy management. Answer, p. 4. The examiner found that it would have been obvious to one having ordinary skill in the art at the time the invention was made to render the policy in HTML or XML format in order to provide a format that is universally viewable across a wide variety of computer platforms and operating systems. Answer, p. 4.

To the extent that the appellants are contesting the examiner's assertion that HTML and XML formats were "well known" at the time of the invention (Brief, p. 16), we note that the specification, on pages 12 and 14, discuss these formats only by type and assume that one skilled in the art would recognize and be able to make and use the invention based on this disclosure. Thus, for the appellants' disclosure to be enabled for use of HTML or XML versions of the policy, it would appear that these formats were within the knowledge of one skilled in the art at the time of the invention. Further, the claims do not recite any particular functionality of these formats other than being human-readable. Thus, applying the same reasoning as set forth *supra* with regard to claim 1, we hold that the recitation of a specific human-readable version of the policy is merely a recitation of non-functional descriptive material, and not entitled to patentable weight.

To the extent that the appellants are challenging the examiner's finding of obviousness, we agree with the examiner that it would have been obvious to one having ordinary skill in the art at the time of the invention, possessed with the teaching in Abraham of generating a human readable version of the policy (see facts 26 and 34) and possessed with the knowledge that the use of HTML and XML protocols are well known in the art, to generate an HTML or XML version of the policy in order to provide a format that is universally viewable across a wide variety of computer platforms and operating systems. *DyStar Textilfarben GmbH v. C.H. Patrick Co.*, 464 F.3d 1356, 1368 (Fed. Cir. 2006) (finding an implicit motivation to combine prior art teachings can be based on the universal "desire to enhance commercial opportunities"). As such, we determine that the examiner made out a prima facie case of obviousness of claims 6, 7, 17, and 18. Accordingly, we sustain the examiner's rejections of these claims under 35 U.S.C. § 103(a).

Claims 10 and 21

The appellants argue claims 10 and 21 as a group. As such, we treat claim 10 as the representative claim. The appellants argue that claim 10 is patentable over the cited references because it claims generating a table of policy elements that have a correlation to the policy statement. The appellants contend that the examiner has failed to make a prima facie showing of obviousness because the cited references do not teach or suggest this step. Brief, p. 17.

We disagree. We do not consider the correlation of a table of policy elements to a policy statement to be a patentable distinction in view of the admitted prior art described in the background of the appellants' own specification, which recognizes that P3P policies consist of statements made using the P3P vocabulary

for expressing privacy practices (see fact 35). Since it was known to express P3P policies as policy statements, it would have been obvious to one having ordinary skill in the art at the time of the invention, in view of the teaching of Abraham to display the policy to an administrator in the form of a table (see fact 27), to have displayed the privacy policy elements to the user in a table where it is known that the privacy policy elements correlate to P3P policy statements. Accordingly, we sustain the rejection of claims 10 and 21 under 35 U.S.C. § 103(a).

Claims 11 and 22

The appellants argue claims 11 and 22 as a group. We treat claim 11 as the representative claim. The examiner found the subject matter of claim 11 obvious in view of Moriconi's teaching of generating a log file, because it was well known within modern computing systems to automate the generation of error reports from log files. Answer, p. 4 (*citing* Moriconi, col. 11, lines 44-46). The appellants argue that there is no teaching or suggestion in the cited references of generating an error statement and that the examiner's reliance on what is "well-known" in the art is improper. Brief, p. 18. We agree with the examiner. We hold that an implicit motivation exists, based on the teaching in Moriconi of maintaining an audit log accessible by the administrator and containing information about authorization requests (see fact 12), and based on the teaching in Moriconi of a parser/type checker to check the policy rules for errors (see fact 11), to record any such errors in a similar audit log for access by the administrator to correct such errors prior to distributing the policy to the client. *In re Kahn,* 441 F.3d 977, 987-88, 78 USPQ2d 1329, 1336 (quoting *In re Kotzab,* 217 F.3d 1365, 1370, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000) ("The test for an implicit showing is what the combined teachings,

knowledge of one of ordinary skill in the art, and the nature of the problem to be solved as a whole would have suggested to those of ordinary skill in the art.") Accordingly, we sustain the examiner's rejection of claims 11 and 22 under 35 U.S.C. § 103(a).

Claim 23

With regard to claim 23, the examiner determined that Moriconi discloses an interface for creating a privacy policy as claimed, except that it does not explicitly disclose a third portion for displaying a privacy policy generated from the groups of data elements. The examiner found that Abraham discloses a third portion for displaying a privacy policy generated from the groups of data elements and further found that it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the method of Moriconi with the method of Abraham in order to secure management of a computer network. Answer, p. 6.

The appellants contend that Moriconi does not teach or suggest an interface having a portion for displaying predefined data elements or a portion for displaying groups of data elements. Brief, p. 18. The appellants further contend that Abraham merely teaches using a graphical user interface to allow a user to input information and does not teach or suggest an interface having a portion for displaying a privacy policy generated from the groups of data elements. Brief, p. 19. The appellants argue that even when the teachings of Moriconi and Abraham are combined, there is still no teaching or suggestion of an interface having the three portions as claimed. Brief, p. 19.

We find that graphical user interface depicted in Figures 6 and 8O of Abraham discloses all of the elements of claim 23 (see facts 28-34). A disclosure that anticipates under 35 U.S.C. § 102 also renders the claim unpatentable under 35 U.S.C. § 103, for anticipation is the epitome of obviousness. *In re Pearson*, 494 F.2d 1399, 1402, 181 USPQ 641, 644 (CCPA 1974); s*ee also In re Fracalossi*, 681 F.2d 792, 794, 215 USPQ 569, 571 (CCPA 1982).

The only difference between Abraham and the claimed interface is that the list of data elements displayed in Abraham contains data elements relating to a security policy instead of a privacy policy. For the same reasons provided above in the discussion of claim 1, we find that this difference is not a patentable distinction over the prior art. Accordingly, we sustain the examiner's rejection of claim 23 under 35 U.S.C. § 103(a).

CONCLUSION

To summarize, the collective teachings of Moriconi and Abraham teach or suggest all limitations of claims 1-24. Even though, in some instances, we sustain the examiner's rejections for different reasons than those advanced by the examiner, our position is still based upon the collective teachings of the references and does not constitute a new ground of rejection. *In re Bush*, 296 F.2d 491, 496, 131 USPQ 263, 266-67 (CCPA 1961); *In re Boyer*, 363 F.2d 455, 458 n.2, 150 USPQ 441, 444 n.2 (CCPA 1966). Accordingly, the decision of the examiner to reject claims 1-24 under 35 U.S.C. § 103(a) is sustained.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

STUART S. LEVY
Administrative Patent Judge

ROBERT E. NAPPI
Administrative Patent Judge

LINDA E. HORNER
Administrative Patent Judge

) BOARD OF PATENT APPEALS AND INTERFERENCES

Gerald R. Woods
IBM Corporation
T8/503
PO Box 12195
Research Triangle Park, NC 27709